APPLICATION

FOR

UNITED STATES LETTERS PATENT

APPLICANT NAME: Bazot et al.

TITLE: METHOD AND SYSTEM FOR ACCESSING INTERNET RESOURCES THROUGH A PROXY USING THE FORM-BASED AUTHENTICATION

DOCKET NO.: FR920020064US1

INTERNATIONAL BUSINESS MACHINES CORPORATION

CERTIFICATE OF MAILING UNDER 37 CFR 1.10

I hereby certify that, on the date shown below, this correspondence is being deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, Box Patent Application, Washington, D.C. 20231 as "Express Mail Post Office to Addressee" Mailing Label No. EV225574561US

on November 24, 2003

Dorothea Rubbone
Name of person mailing paper

Dorothea Rubbone November 24, 2003
Signature Date

METHOD AND SYSTEM FOR ACCESSING INTERNET RESOURCES THROUGH A PROXY USING THE FORM-BASED AUTHENTICATION

Technical field

The present invention relates to an Internet environment wherein a user addresses requests for Internet resources to a proxy which transmits these requests to a content server able to provide the Internet resources, and relates in particular to a method and system for accessing Internet resources through a proxy using form-based authentication.

Background

The service provider market has moved up the value chain from pure connectivity services to deliver value-added and revenue generating services. The business model of a service provider, which was initially driven by minutes of use, is being increasingly replaced by data traffic, generated by users that access either internal services owned and maintained by the service provider itself or external services not maintained by the service provider but accessed through the service provider platform. In addition to growing their customer bases, service providers are now looking to increase the average revenue per user to boost revenues. More compelling services such as content, commerce, and other applications promise higher profit margins, improved customer retention, and greater customer satisfaction. However, managing and distributing these third-party services or content services present significant challenges to service providers. Therefore, the service provider plays a key role since it is the intermediary between the end-user and the internal or external services. Its privileged position allows the service provider to not only provide just "simple" access but added value

services such as security, single sign-on, billing, location, etc. at the condition that it cannot be "bypassed" by the user.

In most cases, external services and partners that provide resources will do it for authenticated users only, meaning that they maintain and enforce the authentication and authorization of these users using their own user registry. Therefore, multiple authentication points may exist thus requiring the end-user to maintain multiple user IDs and passwords, and be prompted to authenticate multiple times in order to be able to access his personalized services. Obviously, this represents a fastidious step for the end-user to enter several times username(s)/password(s) in order to access the Web services. As such, the service provider might loose any credibility towards its end-users if it does not provide a solution to this problem. A solution is to provide a "Single Sign On" feature to their end-users giving them the possibility to use the same User Id and password for all services, whether internal or external, that require authentication. With this feature, user authentication only needs to be done once to access services requiring a user Id and password.

At connection time, the service provider asks the end-user to identify himself as an authorized user by responding to a username/password prompt displayed on the user device in order to give end-users the benefit of personalized services and resources according to the end-users choices and preferences. As already mentioned, these personalized services and resources can be either internal services managed and maintained by the service provider or external services provided by content provider partners.

The service providers and content providers partners have to come to an agreement on how end-user credentials should be passed from the service provider to the partners. The HTTP protocol is the transport protocol used for each communication involved, in one hand in the exchanges between the device being used to access the internal or external services provided by the service provider which is typically a Web browser and the service provider platform, and in other hand between the service provider and its service and the partners. Different techniques exist today such as the Basic HTTP Authentication exchange defined in the HTTP standard, HTTP cookies, customized HTTP headers, etc. These techniques can be used to perform such integration around a single sign-on. Unfortunately, these solutions require business development and cost on each side if partners are to directly trust the authentication done by the service provider platform.

The service provider is the intermediary between the end-user and the internal or external services. Thanks to its privileged position, the service provider uses in most cases an HTTP proxy component deployed in its infrastructure, which all end-users must go through, and which acts as a central authentication point for all end-users who wish to access personalized internal and external services and resources.

Two well known and spread authentication methods on the Internet are the HTTP Basic Authentication and forms-based authentication (e.g., an HTML form sent to the end-user prompting the user to enter a username/password), both over a normal or secure encrypted connection. Although performing single sign-on with Basic Authentication is relatively easy (and most of the HTTP proxies in the market already support single sign-on to back-end application servers representing external services or content provider partners using the HTTP Basic Authentication as

described in the HTTP specification) most servers choose not to use it as a means of authentication, primarily because the user interface is unsophisticated and set by the Web browser and also because it is limited to a single hostname. Forms-based authentication is much more widely used because it is more flexible. Unfortunately, it is this very flexibility that makes single sign-on to form-based systems so difficult to handle insofar as the forms being used are various and different in function of the servers, thereby requiring a development cost.

Summary of the invention

Accordingly, the main object of the invention is to provide a method and a system allowing service providers to reduce the cost of development to perform single sign-on in case of partners using a form-based authentication, thereby avoiding any additional development effort and cost on both sides (service providers and partners).

The invention relates therefore to a method for accessing Internet resources provided by at least a content server in a data transmission system including a proxy connected to the Internet network, the proxy being adapted to perform form-based authentication of a user when receiving a user request for Internet resources therefrom, and wherein the proxy transmits the user request to the content server which sends back a response to the proxy. Such a method comprises the following steps:

-transmission from said proxy to a Single Sign On (SSO) Server of the user request together with credentials associated with the user,

-filling by the SSO server of a login form obtained from the content server, the form being filled using the credentials,

-transmission by the content server to the SSO server of a response to the user request after receiving the filled login form from the SSO server, this response being then sent back to the proxy and,

-transmission by the proxy of the requested information to the user, the information being contained in the response received by the proxy.

According to another aspect, the invention relates to a data transmission system including a proxy connected to the Internet network and at least a content server to which a user can gain access through the proxy, the proxy being associated with authentication means adapted to perform form-based authentication of the user when receiving a user request for Internet resources therefrom and wherein the proxy transmits the user request to the content server which sends back a response to the proxy. The authentication means comprise a Single Sign-On (SSO) server adapted to obtain a login form from the content server when receiving the user request from the proxy, to fill the login form using the credentials associated with the user, and to send back the filled login form to the content server, so that the content server can provide the requested information after authentication of the user.

Brief description of the drawings

The above and other objects, features and advantages of the invention will be better understood by reading the following more particular description of the invention in conjunction with the accompanying drawings wherein:

- Fig. 1 is a schematic block-diagram showing a data transmission system according to the invention.

- Fig. 2 is a schematic block-diagram representing the different data flows achieved between the elements of the data transmission system illustrated in Fig. 1.
- Fig. 3 is a diagram illustrating the flows being achieved for each kind of request transmitted by the user to the proxy in the data transmission system illustrated in Fig. 1.

Detailed description of the invention

Referring to Fig. 1, representing a data transmission system used in the context of the invention, a service provider provides Web services to a plurality of users such as user 10 through the Internet network 12. Such web services can be any kind of information which can be furnished by a content server 14. When the user wants to access the content server, the user transmits a request to a proxy 16. Proxy 16 has at its disposal a user registry (not shown) containing information such as the credentials of the users allowed to access the services provided by the service provider (generally the identification and password of the user).

The proxy 16 is connected to a Single Sign-on (SSO) server 18 which is deployed in the service provider platform in order to recognize when a login form is presented and to interpret it and respond accordingly. For this, the SSO server 18 has at its disposal a configuration file 20 which provides details about signing on to the content server 14. The role of the configuration file 20 is to specify the URL of the login page into the server 14, the location of the login page, the name of the input field used for "username" and the name of the input field used for "password".

In a preferred embodiment of the invention, the SSO Server 18 is an additional component, external to the proxy 16, and does not assume any specific behavior different from the standard behavior that every proxy should implement. However, it could also be closely integrated within the proxy 16 itself, thus providing additional advantages (fewer components, no need for specific service entry point URL) at the additional cost of developing the functionality described in the invention inside it.

The diagram in Fig. 2 illustrates the steps achieved in the method in accordance with the present invention. These steps include the following:

1) The user 10 logs on to the HTTP proxy 16. The user 10 accesses the back-end application service in content server 14 by clicking a specific URL provided by the service provider that identifies the service entry point and references to SSO server 18.

2) Upon reception of this request, the HTTP proxy 16 passes the user's authentication information to the SSO server 18 (e.g., a standard HTTP authorization header credential such as the authorization HTTP header described in the HTTP specification).

3) The SSO server 18 generates a GET request using the information from its configuration file 20, sends it to the content server 14 and obtains the custom login page and any session information such as cookies.

4) The SSO server 18 filters the login form and, using information from its configuration file 20, fills in the

username/password (together with any hidden fields, data, and session cookies).

5) The SSO server 18 generates a POST request and transmits it to the content server 14. The content server 14 authenticates the request and returns the result (plus session information if any) back to the SSO server 18.

6) The SSO server 18 sends the HTTP response and any session information to the HTTP proxy 16.

7) The HTTP proxy 16 forwards this information back to the user 10.

8)-9) All subsequent requests to the content server 14 are routed across the standard junction to the content server 14 (a junction is a configuration rule that exists in the proxy 16 to handle the connection between the proxy 16 and the content server 14).

The data flows corresponding to the different kinds of requests transmitted from the user are represented in Fig. 3.

A. *First request issued by the user*

The user 10 sends the first request to the HTTP proxy 16, invoking the external URL configured in the proxy 16 (/). Since the invoked URL is protected, the proxy 16 sends an authentication challenge to the user 10. Different methods can be used to send this challenge (HTTP response code 401, a form, etc.). This is independent from the authentication technique required by the back-end servers. The user 10 responds with his/her credentials (typically a user name and password). The proxy 16 verifies these credentials against

its user registry, and accepts them if they correspond to a valid user. It returns a HTTP response to the user 10.

B. *Processing of the HTTP request to the content server*

The user 10 now sends a request towards a back-end service in the content server 14. From the invoked URL, the proxy 16 reroutes this request to the SSO server 18, augmented by the user credentials (such as the HTTP Authorization Header) collected in step A. The SSO server 18 will then play the role of the user 10 with regard to the content server 14.

C. *Content server authentication procedure*

The SSO server 18 invokes the login form configured for the content server 14, and the content server 14 responds with the login form. The SSO server 18 "fills in the form", and posts the user credentials to the content server 14. Since these credentials are valid, the content server 14 sends back an HTTP response to the SSO server 18, potentially augmented by a session cookie, specific to the content server 14. The content of this cookie is opaque to the SSO server 18 and to the proxy 16, and will allow the content server 14 to verify, on subsequent requests, that this user 10 has been properly identified. Cookies are important in a form-based login environment because they are often used by the server to identify the user's session. Obviously, precautions have to be taken around the Internet domain and the cookies, because a cookie will be replayed by a Web browser if it matches the Internet domain of the HTTP requests submitted. Optionally this response can be combined with a redirection towards the content server 14, which will allow subsequent requests to flow directly either from the proxy 16 to the content server 14, bypassing the SSO Server 18, or from the user 10 directly

to the content server 14. The SSO server 18 forwards this response back to the proxy 16, and then to the user 10.

D. *Subsequent requests*

The proxy 16 forwards subsequent requests directly to the content server 14, without going through the SSO server 18. In each request the user repeats the content server 14 session cookie (if any), which is used by the content server 14 to retrieve the user context.

The foregoing description of the preferred embodiments of this invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed, and obviously, many modifications and variations are possible. Such modifications and variations that may be apparent to a person skilled in the art are intended to be included within the scope of this invention as defined by the accompanying claims.